UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,089	06/25/2003	Brian S. Christian	MS1-1512US	4285

22801 7590 01/04/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	01/04/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/04/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/606,089	CHRISTIAN ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-12,16-21 and 24-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-12,16-21 and 24-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/22/2006 has been entered.

This action is in response to the communication filed on 9/22/2006.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 4-12, 16-21, and 24-28 are pending.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Regarding claims 1, 12, and 21, Applicant has not pointed out where the amended claim is supported, nor does there appear to be a written

description of the claim limitation *'wherein one or more predetermined symbols are removed without replacement from the data input'* in the application as filed."

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 1, 4-12, 16-21, and 24-28 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, support is lacking for the new limitations, recited within claims 1, 12, 21, as filed. See above objection to the specification.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 21 and 24-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 21 and 24-28 pertain

to carrier waves bearing instructions. Claims reciting a signal encoded with descriptive material fails to fall within any of the categories of patentable subject matter set forth in 35 USC § 101.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-12, 16-21, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (Scott), "Abstracting Application-Level Web Security" in view of Wheeler, Secure Programming for Linux and Unix HOWTO.

Regarding claim 1, Scott discloses:

receiving data input through a web page from a client device (fig. 1, page 2, col. 1, par. 3-6); *referencing a declarative module to determine a client input security screen to apply to the data input from the client device* (page 3, col. 2, par. 2);

wherein the declarative module comprises:

a global section that includes at least one client input security screen that applies to any type of client input value (fig. 2; page 6, col. 1, par. 1, 2, par. 2, lines 9-13). Scott

discloses input security screens (i.e. a transformation screen) that are applied to all user input (parameters values);

an individual values section that includes at least one client input security screen that applies to a particular type of client input value (fig. 2; page 4, col. 1). Herein, Scott discloses screens for screening particular types of client input values (i.e. cookies, urls, other parameters). Thus Scott discloses an individual values section.

and applying multiple client input security screens to the data input from the client device (page 3, col. 2, par. 2; fig. 2), *including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module, wherein the client input security screens are distinct from one another* (page 3, col. 2, par. 1, 2; fig. 2). Herein, Scott discloses separate screens.

Scott discloses the application of a plurality of validation and transformation screens to the input data of a client. The system of Scott thus provides protection against security attacks, for example - malicious scripting attacks as revealed by CERT Advisory [CA-2000-02] (Scott, pg. 2, "Cross-Site Scripting"). However, regarding such validation and transformation screens, Scott does not explicitly state *wherein one or more predetermined symbols are removed without replacement from the data input.*

Nevertheless, the examiner points out that when protecting against security attacks, such as malicious scripting attacks, the notion of [*removing*] *one or more predetermined symbols...without replacement from the data input* was well known to those ordinary skill in the art. Applicants may refer to their own admission of such.

Specifically, Applicants state that prior art systems combat security attacks by "discarding" (removing without replacing) or "altering" (removing and replacing) one or more predetermined symbols (Instant Application, par. 6).

Similar to Scott, Wheeler discloses security methods to validate and transform client input data so as to protect against the types of security attacks as revealed by CERT Advisory [CA-2000-02] (Wheeler, 6.15.1:"Explanation of the Problem"; 4:"Validate All Input; 6.15:"Prevent Cross-Site Malicious Content – 6.15.2-3:"Identifying Special Characters", "Filtering", "Encoding"). Wheeler discloses as advantageous, that when preventing security attacks, a system should perform the methods of filtering data (removing), encoding data (removing and replacing), and validating data (allowing only valid data to pass) (Wheeler, 6.15.2, "Solutions to Cross-Site Malicious Content").

It would have been obvious to one of ordinary in the art to employ the method *wherein one or more predetermined symbols are removed without replacement from the data input* as taught by Wheeler within the system of Scott. This would have been obvious because one of ordinary skill in the art would have been motivated by the advantages of security and flexibility to incorporate the various well known and suggested methods taught by Prior art as being effective against security attacks.

Regarding claim 4, the combination discloses:

wherein the particular type of client input value is one of the following types of client input values: query string; server variable; form value; cookie (Scott, fig. 2).

Regarding claim 5, the combination discloses:

wherein the declarative module further comprises a web.config file (Scott, page 1, col. 2, par.3; page 3, col. 2, par. 1).

Regarding claim 6, the combination discloses:

wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen (Scott, page 3, col. 2, par. 1, lines 8-13, par. 2, lines 5-11; page 4, col. 2, par. 3,4). Scott discloses the application of several types of input screening to all input data (default screening) wherein actions are performed on the all the input data during the process of data input security screening. Additionally, Scott discloses default transformations that can be applied during the screening of invalid input data.

Regarding claim 7, the combination discloses:

wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen (Scott, page 4, col. 1, par. 4-6).

Regarding claim 8, the combination discloses:

wherein a client input security screen further comprises one or more values that may be entered as client input, the one or more values further comprising the only

values that may be entered as client input (Scott, page 4, col. 1, par. 4-6). Scott discloses a security screen that constrains client input to a set of values, such as any integer: 0 – int [length 4]. Thus, the security screen effectively comprises the values of 0 – int [length 4] to be imposed upon the client input as a restriction. Additionally, Scott discloses that the security screen comprises specific URL values (extracted from HTTP requests) that may be entered as client input (Scott, page 6, col. 2, par. 1).

Regarding claim 9, the combination discloses:

wherein a client input security screen further comprises one or more screened values that, when detected in the client input, cause an action to be taken on the client input (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3).

Regarding claim 10, the combination discloses:

wherein the action to be taken further comprises removing the one or more screened values detected in the client input (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3, 4). Scott discloses the encoding of screened values (removal and replacement). Additionally, Scott discloses the removal of values from client input based upon the client input security screen (Scott, page 7, col. 2, par. 1.1 – 1.2)

Regarding claim 11, the combination discloses:

wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input (Scott, page 6, col. 2, par. 3; fig. 5; page 9, col. 1, par. 2.2).

Regarding claim 12, it is the system claim corresponding to the method claim 1, and is rejected for, at least, the same reasons, and furthermore because Scott discloses:

a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network (Scott, fig. 1).

Regarding claim 16, the combination discloses:

wherein a screening rule further comprises a client input variable that may be accepted as input from a client (Scott, fig. 5). Scott discloses various screening rules that accept client input variables.

Regarding claim 17, the combination discloses:

wherein a screening rule further comprises one or more screened characters that, when detected in client input, are screened from the client input according to a screening rule (Scott, fig. 5 – see transformation).

Regarding claim 18, the combination discloses:

wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action (Scott, fig. 5 – see transformation). Scott discloses a single screening action that is to be performed, and thus, a default screening action.

Regarding claim 19, the combination discloses:

wherein the screening rule further comprises a specified screening action that is applied to the screened client input (Scott, fig. 5 – see transformation). Scott discloses a single specific screening action that is to be performed.

Regarding claim 20, it is rejected, at least, for the same reasons as claim 5.

Regarding claim 21, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination discloses:

serving a web page to a client over a distributed network; receiving client input via the web page (Scott, fig. 1, page 2, col. 1, par. 3-6)*; comparing the client input with multiple and distinct client input security screens stored in a security declarative module; wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values* (see rejection of claim 1)*; if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module* (Scott, page 3, col. 2, par. 2; page 4, col. 2, par. 3; page 6,

col. 1, par. 1, 2; fig. 5)*; and wherein the client input security screens included in the security declarative module can be applied to multiple web pages* (Scott, page 4, col. 1, par. 2).

Furthermore, Scott discloses a computer system, and thus discloses media and instructions (Scott, fig. 1).

Regarding claims 24 and 25, they are the media and instruction claims corresponding to the method and system claims of 5 – 7, 18, and 19, and they are rejected for, at least, the same reasons.

Regarding claim *26*, the combination discloses:

wherein the screening action further comprises a default action that is not required to be specified in a client input security screen (Scott, page 6, col. 1, par. 1, 2).

Regarding claims *27* and 28, the combination discloses:

wherein the multiple web pages are included in a web project and *wherein the multiple web pages are included in a web-based application* (Scott, Abstract; Introduction; fig. 1; section 3.1; page 4, col. 1, par. 2; page 6, col. 1, par. 2, col. 2, par. 1). Scott discloses a security policy to be applied to a large web-application, the policy comprising rules for the web pages of a site. The web pages are associated with a web application, thus, they are included in a web project/application.

Response to Arguments

Applicant's arguments with respect to the above rejected claims have been considered but are moot in view of the new ground(s) of rejection.

Furthermore, Applicant's arguments filed 9/22/2006 have been fully considered but they are not persuasive.

Applicants argue primarily that:

(i) Furthermore, Scott is completely lacking ...the subject matter of claim 1. The immediately foregoing deficiency of Scott has been argued previously in the prosecution of this matter and is not reiterated here in the interest of brevity.

In response, the examiner respectfully refers the applicant to the examiner's previous responses to such argument and any such similar argument regarding the screening of all input and the screening of individual types of input.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited.

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams
AU: 2137

JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER